UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

KRIPTOGRAFIJA IN RAČUNALNIŠKA VARNOST

Seminarska naloga

E-Glasovanje

Avtor:
David Vidrih

Ljubljana, 2004

KAZALO

1. UVOD

Cilj tega dokumenta je predstaviti E-Glasovanje, njegove sheme in njihovo ustreznost ter I-Glasovanje (glasovanje prek Interneta) in njegovo izvedljivost danes.

E-Glasovanje je izražanje volje volivcev z uporabo elektronskih naprav, kar naj bi glasovanje poenostavilo, naredilo bolj pravično, ter skrajšalo čas in stroške volitev.

Prva tri poglavja so namenjena predstavitvi osnovnih konceptov in problemov izvedbe idealnih demokratičnih volitev. Razumevanje teh konceptov je nujno potrebno za razumevanje glavnega dela besedila. Ta tri poglavja vsebujejo definicijo osnovnih pojmov, pregled sistemov za glasovanje skozi zgodovino in pregled problemov glasovanja.

Glavni del besedila, četrto in peto poglavje, sestavljata opis oziroma ovrednotenje kriptografskih volilnih modelov in shem ter študija možnosti izvedbe glasovanja preko Interneta. Sledi še kratek pregled razvoja, uvajanja in uporabe E-Glasovanja po svetu.

Za konec je podan povzetek trenutnega stanja in aktualnih problemov ter napovedi za prihodnost.

1.1. Glasovanje

Volitve definiramo takole [5] :

Glasovanje oziroma volitve so proces v katerem ljudje izražajo svojo izbiro oziroma želje.

V volitvah sodelujejo volivci in volilne oblasti. Volivci so osebe, katerim je z zakonom ali določili dovoljeno glasovati. Oblast pa vodi volitve oziroma izvaja volilni proces. Oblast je ponavadi sestavljena iz predstavnikov različnih strani, od katerih vsaka zagovarja nič (neopredeljenost), enega ali več izidov glasovanja. S tem naj bi bila dosežena korektnost volitev.

Volitve delimo na različne načine, najpomembnejša sta dva. Prvi je **teža glasu posameznika**, ta je pri večini volitev enaka za vse udeležence, lahko pa je različna glede na položaj posameznikov. Različne teže oziroma pomembnosti predstavimo z utežmi. Druga delitev pa se nanaša na **obliko glasu**, sledi nekaj primerov:

- da/ne volitve – odločamo se za ali proti neki stvari oziroma trditvi
- 1-od-*L* volitve – izberemo eno od *L* možnosti
- *K*-od-*L* volitve – izberemo *K* od *L* možnosti
- 1-*L*-*K* – najprej izberemo eno od *L* skupin, nato pa iz te skupine izberemo *K* možnosti

- strukturirane volitve – imamo *n* nivojev možnosti, na *i*-tem nivoju izberemo k_i možnosti
- pisna oblika volitev – formuliramo in zapišemo svoj odgovor, ki ne sme biti daljši od določene dolžine

Množično glasovanje, npr. na državni ravni, je ponavadi razdeljeno v regijsko hierarhijo.

1.2. Proces glasovanja

Celoten proces glasovanja je tradicionalno sestavljen iz štirih zaporednih faz [4]:

1. **Vzpostavitev volitev**
   Oblasti morajo napovedati volitve, formulirati vprašanje glede katerega se bodo volivci odločali, organizirati izvedbo volitev in izdelati register volivcev. Register volivcev je seznam oseb, ki imajo pravico voliti.

2. **Preverjanje volivca**
   Osebo, ki pride na volitve je treba identificirati, ali sploh lahko voli in označiti, da je prišla voliti. S tem dosežemo en glas na legalnega volivca.

3. **Dejansko glasovanje**
   Volivec glasuje tako, da izpolni glasovnico. To mora imeti možnost narediti tako, da nobeden ne vidi njegove odločitve. Možnost ima tudi oddati prazno oziroma neizpolnjeno glasovnico. Izpolnjeno glasovnico odda v skrinjico z glasovi, kjer se pomeša z glasovi drugih volivcev. Oblika glasovnice je odvisna od načina volitev, natančneje od same fizične izvedbe glasovanja.

4. **Določanje rezultata volitev**
   Rezultat volitev ugotavljajo oblasti po uradnem koncu glasovanja. Takrat odprejo skrinjice z glasovi in preštejejo glasove. Ko so vsi glasovi prešteti, objavijo uraden rezultat volitev.

Druga in tretja točka potekata skupaj, zato sta včasih združeni v eno samo fazo 'volitve'.

1.3. E-Glasovanje - elektronsko glasovanje

E-Glasovanje je okrajšava za elektronsko glasovanje, kar pomeni izvedbo volitev s pomočjo oziroma podporo elektronskih sistemov.
Le-ti so v splošnem lahko uporabljeni le v nekaterih ali v vseh fazah in podfazah procesa glasovanja. Celovita elektronska podpora bi pomenila oddajo glasu preko neke elektronske naprave, pa naprej preko zagotavljanja vseh zahtevanih lastnosti glasovanja do ugotavljanja in objave rezultatov glasovanja.
E-glasovanje ima določene prednosti in slabosti, vendar o tem ne moremo govoriti, preden elektronskega glasovanja ne ločimo od I-Glasovanja oziroma internetnega glasovanja.

1.4. Oddaljeno glasovanje

To je glasovanje, ki se ne vrši na voliščih, ampak iz nekih drugih oddaljenih lokacij. Primeri oddaljenega glasovanja so glasovanje preko pošte, telefona ali Interneta. Oddaljeno glasovanje ima veliko dobrih lastnosti (volivcem ni treba na volišče, svoj glas lahko oddajo od kjerkoli…). Po drugi strani pa, ravno zaradi oddaljenosti, ni pod nadzorom oblasti in imamo zato kup dodatnih problemov (razni napadi z namenom onemogočanja oddaje glasu ali spreminjanja glasu volivca). Prednosti in problemi bodo podrobneje predstavljeni v nadaljevanju.

1.5. I-Glasovanje - glasovanje preko Interneta

I-Glasovanje je le posebna vrsta oddaljenega elektronskega glasovanja. To je glasovanje, v katerem volivci oddajo svoj glas preko Interneta.
Seveda to ne more biti edina možnost glasovanja, saj vsi ljudje nimajo dostopa do Interneta in je tako ta izvedbeni tip glasovanja nujno treba kombinirati z drugimi, tradicionalnimi izvedbeni tipi glasovanja.
Glavna razlika I-Glasovanja od drugih elektronskih in tradicionalnih izvedbenih tipov glasovanja je, da je to oddaljeno glasovanje. Največja prednost I-Glasovanja je predvsem to, da volivcu ni treba na volišče, ker lahko glasuje kar od doma, iz službe oziroma kjerkoli iz Interneta.
I-Glasovanje pa odpre tudi cel kup problemov. Ker volivec ne oddaja svojega glasu pod nadzorom oblasti, ga lahko kdo nadzoruje oziroma prisili, da glasuje po želji izsiljevalca. Možno je tudi kupovanje glasov, saj lahko 'kupec' vidi, kako bo volivec glasoval. Poveča se problem družinskega glasovanja. Problemi glasovanja so podrobno pojasnjeni v tretjem poglavju.
Druga množica problemov lahko nastane zaradi same uporabe Interneta. Treba je zagotoviti varnost in tajnost prenesenih podatkov, treba je zagotoviti dovolj dobre povezave in kapacitete, preprečiti vse možne napade in podobno.
Pri neoddaljenih elektronskih načinih glasovanja, kjer je vsa oprema in celoten proces glasovanja ves čas pod nadzorom oblasti, zgoraj omenjeni problemi odpadejo. Več o problemih I-Glasovanja v poglavju o izvedljivosti I-Glasovanja danes.

1.6. Zahteve glasovanja

Dobra volilna shema mora zadoščati določenim zahtevam. Osnovne zahteve glasovanja so naslednje [2][3]:

- **Natančnost**
  Sistem glasovanja je natančen, če:
  - ni možno spremeniti glasu,
  - ni možno izvzeti glasu iz končnega preštevanja,
  - ni možno štetje neveljavnega glasu pri končnem preštevanju.

Napake mora biti možno vsaj zaznati, če že ne odpraviti. Sistemi, pri katerih je možno napake odpraviti imenujemo *natančne*, tiste, pri katerih je mogoče napake le zaznati, pa *delno natančne*.

- **Demokratičnost**
  Sistem glasovanja je demokratičen, če:
  - zagotavlja možnost glasovanja vsem, ki imajo pravico glasovati,
  - zagotavlja, da lahko vsakdo, ki ima pravico glasovati, glasuje največ enkrat.

- **Zasebnost**
  Sistem glasovanja je zaseben (privaten), če
  - ne oblasti, ne nihče drugi ne more povezati glasu volivca z volivcem samim,
  - noben volivec ne more dokazati kako je volil.

  Zasebnost zagotovimo z **odsotnostjo potrdila**, kar pomeni, da volivec ne sme v volilnem procesu imeti možnosti pridobiti nobenega potrdila s katerim bi lahko nekomu dokazal kako je volil. S tem se prepreči kupovanje glasov in izsiljevanje.

- **Preverljivost**
  Sistem glasovanja je preverljiv, če lahko kdorkoli neodvisno preveri ali so bili vsi glasovi pravilno upoštevani.
  To je zahteva, ki bi jo moral imeti vsak volilni sistem, če pa to ni možno, potem naj bi vsaj posamezni volivci imeli možnost preveriti pravilnost upoštevanja njihovega glasu, pri čemer spet ločimo možnost zaznavanja napake in možnost odpravljanja napake. Še slabša verzija omogoča preverljivost le oblastem.
  Preverljivost je zelo šibka točka tradicionalnih volilnih sistemov.

- **Prikladnost**
  Sistem glasovanja je prikladen, če omogoča volivcem oddajo svojega glasu hitro, enostavno, v eni seji (navzočnost volivca je potrebna le enkrat) in če ne zahteva posebnih znanj in sposobnosti.

- **Fleksibilnost**
  Sistem glasovanje je fleksibilen, če omogoča različne tipe in oblike glasovanja, kateri so našteti zgoraj pod opisom glasovanja.

- **Mobilnost**
  Sistem glasovanja je mobilen, če ni nobenih ovir glede lokacije, iz katere volivec odda glas. To je v sodobnem svetu, ko so ljudje vedno bolj mobilni, zmeraj bolj pomembno.

Kasneje bomo pri obravnavi izvedljivosti I-Glasovanja spoznali še dve specifični zahtevi: **infrastruktura** in **zlonamerna koda**.

Tradicionalne volitve seveda še zdaleč ne ustrezajo tem zahtevam, luknje imajo na vseh koncih in krajih. Opis vseh teh lukenj se nahaja v tretjem poglavju (problemi glasovanja). Med probleme oziroma luknje tradicionalnega glasovanja spadajo vsi tam opisani problemi, razen tistih, ki se nanašajo na oddaljeno glasovanje.

2. SISTEMI ZA GLASOVANJE SKOZI ZGODOVINO

To poglavje obsega kratek pregled sistemov oziroma naprav za glasovanje, kateri so bili uporabljeni skozi zgodovino. Namen predstavitve je le na kratko prikazati razvoj sistemov za glasovanje. Predstavitev je pomembna za razumevanje današnjega stanja na področju glasovanja in elektronskega glasovanja.

Časovno si sistemi sledijo takole [1]:

- **Papirnate glasovnice**
  Glasovnico je predstavljal list papirja, da katerem so bila vprašanja oziroma kandidati, zraven njih pa prostor, na katerega so volivci zapisali oziroma označili svojo odločitev. Papirnato glasovnico so volivci oddali v zapečateno volilno skrinjico. Po poteku možnega časa za oddajo glasov so oblasti odprle te skrinjice in preštele glasove.
  Štetje glasov je pri tem sistemu zelo zamudno in podvrženo človeškim napakam.

- **Naprave z mehanskimi ročicami**
  Taka naprava je imela toliko ročic, kolikor je bilo kandidatov oziroma izbir. Vsaki izbiri je bila prirejena ena ročica, ob njej je bila ta izbira tudi zapisana. Naprava je imela tudi posebno ročico, ki je pripravila napravo za začetek oddaje glasu. Ob aktiviranju te ročice so se vse izbirne ročice postavile v nevtralen položaj, hkrati pa se je zagrnila tudi zavesa, ki je omogočala zasebnost volivca. Volivec je za oddajo glasu potegnil ustrezne ročice. V napravi so bili mehanski števci, podobni avtomobilskim, ki so šteli število glasov za vsako izbiro. Ti števci so se na začetku volitev nastavili na nič. Po povečanju števca ustreznega volivčevi izbiri, je naprava postavila vse izbirne ročice nazaj v nevtralen položaj. Notranji mehanizmi so preprečevali volivcu izbrati več možnosti, kot je bilo dovoljeno in oddajo več kot enega glasu. Rezultat volitev so enostavno odčitali iz števcev.
  Štetje glasov je avtomatizirano in tako bolj zanesljivo kot pri ročnem štetju papirnatih glasovnic.

- **Luknjane kartice**
  Pri sistemu luknjanih kartic volivci dobijo kartico in posebno napravo za luknjanje kartic. Volivci z omenjeno napravo preluknjajo prejeto kartico ob izbiri, za katero so se odločili. Preluknjano kartico oddajo v volilno skrinjico ali pa računalniško vodeni napravi za štetje glasov.
  Problem tega sistema je, da volivci včasih z temi napravami za luknjanje kartic niso naredili idealne luknje, ampak se je majhen krogec kartice še zmeraj držal kartice. Ta držeči se krogec je dobil svoje ime (chad) in kategorizacijo glede na to koliko se je še držal kartice. To je seveda zelo zapletlo preštevanje takih glasov. Poleg kartice in naprave za luknjanje so volivci dobili še navodila, iz katerih je bilo razvidno, kje narediti luknjo za določeno izbiro; na karticah namreč niso bile vedno izpisane tudi izbire, ampak samo oznake. Luknjane kartice je sicer izumil Herman Hollerith za statistične izračune.

Kljub temu, da zgleda sistem zelo zapleten in nekako nestabilen se je v Ameriki veliko uporabljal in se še uporablja.

- **Zaznava oznak (optično skeniranje)**
  Volivci dobijo papirnato glasovnico, na kateri je ob vsaki zbiri prazen kvadrat, ali kaj podobnega. Volivec izbere možnost tako, da v ustrezen kvadrat nariše ustrezno oznako (križec, kljukico, piko…). Tako izpolnjeno glasovnico odvisno od konkretne izvedbe odda v glasovno skrinjico ali pa direktno računalniško vodenemu čitalcu takih oznak. Čitalec oznak skupaj z računalnikom deluje na principu logike temne oznake, in izbere tisto možnost, pri kateri v ustreznem kvadratu zazna največjo temno oznako. Zaznava oznak je le eden od načinov za razpoznavo oznak.

- **Direct Recording Electronic (DRE)**
  Temu bi slovensko rekli 'elektronika za direktno snemanje'.
  Ta sistem je elektronska verzija naprav z mehanskimi ročicami. Pri teh napravah imamo ponavadi zaslon, na katerem so izpisane izbire, namesto ročic pa imamo tipke ali gumbe ali kar zaslon občutljiv na dotik. Glasovi se shranjujejo v pomnilniku naprave.

Vse te naprave so bile razvite najprej v Združenih Državah Amerike, ki imajo od celega sveta najbolj slikovite in razgibane volitve in vse kar spada zraven. Kot zanimivost je v nadaljevanju podana tabela, ki prikazuje uporabo posameznih vrst naprav v ZDA leta 1996:

Sistem	*papirnate glasovnice*	*naprave z mehanskimi ročicami*	*luknjane kartice*	*zaznava oznak*	*DRE*
Prva uporaba	1889	1892	1964	?	?
Procent uporabnikov leta 1996 na predsedniških volitvah	1.7%	20.7%	37.3%	24.6%	7.7%

V Ameriki je bilo v 70ih letih zelo popularno izdelovati naprave za glasovanje. Oblasti več ali manj niso imele nobenih standardov ali meril za testiranje teh naprav ampak so se zanašale bolj na besedo proizvajalcev teh naprav.

3. PROBLEMI GLASOVANJA

Problemov pri glasovanju je ogromno, razdelimo jih lahko v več skupin:

- osnovni problemi
- problemi preprečevanja goljufanja
- problemi oddaljenega glasovanja

3.1. Osnovni problemi

Vsi volivci morajo imeti enake možnosti udeležbe in sodelovanja na volitvah. Posebno pozornost je treba posvetiti predvsem:

- **Jasnost vprašanja glasovanja**
  Vprašanje, na katerega odgovarjajo volivci mora biti jasno in nedvoumno formulirano. To se morda na prvi pogled ne zdi problematično, ampak v praksi se velikokrat zgodi, da je vprašanje slabo zastavljeno in ga volivci ne razumejo. Vprašanje mora biti nedvoumno razumljivo volivcem vseh starosti, vseh stopenj izobrazbe, vseh kultur…

- **Enakopravnost, enake možnosti vsem**
  Generalno moramo zagotoviti, da imajo vsi enake možnosti, ne glede na starost, sposobnosti, izobrazbo…

- **Starejši ljudje**
  Treba je paziti, da v procesu volitev niso uporabljeni kakšni posebni postopki oziroma tehnologija, katera bi lahko delala probleme starejšim občanom. Dober primer za to je že I-Glasovanje, ki vključuje računalnike oziroma Internet, ki še ljudem srednje starosti dela probleme, kaj še starejšim ljudem.

- **Ljudje s posebnimi potrebam**
  Posebno pozornost zaslužijo ljudje, ki ne vidijo, slišijo, ne znajo pisati ali brati oziroma iz kakršnegakoli razloga ne zmorejo določenih zahtevanih opravil procesa glasovanja. Take probleme rešujemo na razne načine, kot so na primer avdio predvajanje volilnega vprašanja, posebne tipkovnice za slepe…

- **Razne politične manipulacije**
  Za zagotavljanje korektnosti volitev je treba, poleg zagotavljanja korektnosti ožjega procesa volitev, preprečevati še vrsto različnih manipulacij pred in med volitvami, kot npr. preverjanje in ukrepanje ob kršenju pravil volilne kampanje in volilnega molka. Zelo problematične so tu lahko zmanipulirane raziskave javnega mnenja. Še bolj kritična pa je lahko objava delnih rezultatov, tako pravilnih, kot ponarejenih, saj ta lahko vpliva na odločitve volivcev.

3.2. Problemi preprečevanja goljufanja

To so problemi preprečevanja goljufanja oziroma poseganja ene strani v proces volitev z namenom izboljšanja izida volitev v prid te strani:

- **Kupovanje glasov, izsiljevanje, družinsko glasovanje**
  Kupovanje glasov je dogovor med kupcem glasu in volivcem, da bo volivec glasoval po naročilu tega kupca, za kar bo od njega dobil dogovorjeno plačilo.
  Do izsiljevanja pride, ko izsiljevalec od volivca izsiljuje, naj glasuje po izsiljevalčevi volji.
  Družinsko oziroma skupinsko glasovanje pa pomeni, da cela družina (oziroma neka skupina) glasuje kot nekdo iz te skupine, bodisi zaradi neopredeljenosti, bodisi zaradi podrejenosti ali že prej omenjenega izsiljevanja.
  Vse te tri načine manipulacije volivcev se da preprečiti z zahtevo po zasebnosti, po kateri nobeden ne more povezati volivca z njegovi glasom. Tudi, če zagotovimo zasebnost, gre pri vseh teh oblikah še vedno za določeno mero pritiska na volivce.

- **Možnost preverjanja pravilnosti upoštevanja glasov**
  Kljub problemom prejšnje točke, pa moramo še vedno zagotoviti možnost preverjanja pravilnega upoštevanja glasov. Poleg generalnega neodvisnega preverjanja, moramo tudi vsakemu volivcu omogočiti preverjanje pravilnosti upoštevanja njegovega glasu. Kako to izvesti, bo vidno v opisih konkretnih shem elektronskih volitev.

- **Problem oblasti z nepoštenimi nameni**
  Kot smo že rekli, je dobro, da je oblast, ki izvaja proces volitev, sestavljena iz predstavnikov različnih strani in neodvisnih predstavnikov. Recimo, da oblast sestavlja N predstavnikov. Potem mora dobra shema volitev to upoštevati in zagotavljati vsaj zaznavanje, če že ne odpravljanje nepravilnosti ob predpostavki, da ima t od teh N oblasti slabe namene [5].
  Pod nekorektno obnašanje oblasti se šteje uničevanje glasov, izraba glasovnic volivcev, ki se volitev niso udeležili, napačno štetje glasov, označevanje glasovnic… Zelo znan je Hitlerjev primer označevanja glasovnic: kdor je volil proti njemu, je bil odstranjen.

- **Večkratna registracija volivcev pod različnimi imeni**
  Volivec lahko informacijo, da nekdo ne bo šel na volitve, izkoristi tako, da gre pod njegovo identiteto še enkrat na volitve. Dogajalo se je že tudi, da so, zaradi napačnih volilnih registrov, volili mrtvi ljudje (nekdo je to izkoristil in oddal glas namesto njih).
  Vsem tem problemom se lahko izognemo s pravilnimi registri volivcev, z pravilno identifikacijo oseb, ki pridejo na volišče in pravilnim beleženjem volivcev, ki so že volili.

- **Nepravilno delovanje naprav za glasovanje in štetje glasov**
  Pri glasovanju so se in se še vedno uporabljajo razne naprave, od preprostega luknjanja kartic do bodočih sistemov za oddaljeno glasovanje.
  Podobno velja za naprave za avtomatsko štetje glasov.
  V praksi se je pokazalo, da mehanski in elektronski sistemi niso stoodstotno zanesljivi in da se lahko pokvarijo.
  Take napake mora biti mogoče zaznati in takoj odpraviti. Na voljo mora biti tudi rezervna oprema, katera enostavno in nemudoma zamenja nepravilno delujočo opremo.

- **Problemi I-glasovanja**
  Ti problemi so že bili nakazani v uvodu pri definiciji I-glasovanja, natančneje pa bodo obravnavani v petem poglavju (izvedljivost I-glasovanja).

3.3. Problemi oddaljenega glasovanja

Problemi oddaljenega glasovanja so problemi, ki izhajajo iz same narave oddaljenega glasovanja [3]:

- **Odsotnost nadzora oblasti**
  Oddaljeno glasovanje ne poteka pod nadzorom oblasti, zato je nevarnost kupovanja glasov, izsiljevanja in družinskega glasovanja še večja. Pri glasovanju pod nadzorom oblasti, oblasti preverjajo identifikacijo in nadzorujejo, da volivec glasuje in odda svoj glas zasebno. Če pa glasujemo oddaljeno, npr. od doma, pa lahko izsiljevalec ali kupec glasov nadzoruje volivčeve akcije. Brez biometrične identifikacije (na primer identifikacija z gesli), lahko nekdo to identifikacijo pridobi in tako lahko izvede volilni proces kar za druge, na primer celo družino.

- **Varovanje podatkov**
  To je problem varovanja vseh podatkov in komunikacijskih poti glasovalnega procesa. Sem spadajo identifikacijski podatki in glasovnica volivca, vse komunikacijske poti…

- **Identiteta in anonimnost volivca**
  Po eni strani moramo biti prepričani, da je glasovnica, katero oblasti dobijo oddaljeno od nekoga, res veljavna in da ima ta oseba pravico voliti in da glasuje samo enkrat… Po drugi strani pa moramo zagotoviti anonimnost, torej ne sme biti možno povezati volivca in njegovega glasu.
  To sta si dve zelo nasprotujoči zahtevi, še posebej pri oddaljenem glasovanju, kjer se da povezavo med volivcem in njegovim glasom ugotovili iz komunikacijskih poti.

- **Odpovedi komunikacij**

Oddaljene komunikacijske poti niso vedno stoodstotno na voljo. V času volitev, natančneje v času možnosti oddaljene oddaje glasov, morajo imeti volivci vsaj vnaprej določen večji del tega časa na voljo komunikacijske poti.

- **Kapaciteta infrastrukture**
  Kapaciteta infrastrukture za podporo oddaljenemu glasovanju mora biti zadostna, da ne pride do preobremenitev in zastojev. Predvsem se je treba zavedati, da se glasovanje izvaja preko neke obstoječe infrastrukture (telefon, Internet…), ki je morda dovolj za navadno uporaba teh storitev, v času oddaje glasov pa bo naval veliko večji, saj bo v relativno kratkem času to infrastrukturo uporabila velika večina uporabnikov hkrati.
  Kapacitete je treba načrtovati in upoštevati tudi določen varnostni faktor.

- **Razni napadi**
  Tu so mišljeni razni možni napadi, kot na primer namerna preobremenitev infrastrukture z namenom onemogočanja oddajanja glasov, zlonamerna koda… Več o tem bo povedano v poglavju o izvedljivosti I-Glasovanja danes.

  Analiza tradicionalnih volitev spet pokaže, da so v bistvu zelo slabo zasnovane in ne rešujejo naštetih problemov. Tako sploh ne ustrezajo zahtevam, ki bi jih volitve morale izpolnjevati.

4. KRIPTOGRAFSKI VOLILNI MODELI IN SHEME

V prejšnjih poglavjih je bilo predstavljeno glasovanje, njegov razvoj in njegovi problemi. Dandanes niti v teoriji, ne obstaja idealen sistem volitev, v praksi pa se še vedno uporabljajo zelo zastareli sistemi.
Zato se veliko dela in raziskuje z namenom izdelati čimbolj idealen volilni sistem. Zaradi svoje narave in zaradi možnosti, ki jih ponuja elektronika in računalniki, gredo raziskave pretežno v računalniške vode. Veliko se uporablja kriptografija. Z drugimi besedami to pomeni, da bodo sodobni volilni sistemi delali na elektronski oziroma računalniški opremi in uporabljali kriptografijo.

V tem poglavju pa bo govora o konkretnih modelih procesa elektronskega glasovanja, o njihovih prednostih, slabostih in ustreznosti zahtevam.
Na začetku bosta predstavljena dva enostavnejša modela, na katerih bo prikazano kako dobro pokrivata vse zahteve volitev in vse njune slabosti.
V nadaljevanju pa bodo predstavljeni drugi bolj resni modeli in sheme z po enim primerom. Ti resni modeli in pripadajoče sheme se delijo v tri skupine:

- sheme na osnovi **slepega podpisa** in **anonimnega kanala,**
- sheme na osnovi **homomorfne kriptografije** (in **deljenja skrivnosti**),
- sheme na osnovi **mešanja glasov.**

4.1. Dve enostavni shemi

Predstavljeni bosta dve relativno enostavni shemi [2]. En namen te predstavitve je prikaz, kako naj bi shema sploh izgledala. Drugi namen pa je pokazati, kako v navidez brezhibni shemi hitro najdemo velike napake in luknje.

4.1.1. Enostavna shema

Shema je predstavljena z spodnjo sliko:

Slika 1: Enostavna shema

V tej shemi poleg volivca nastopa še oblast, katero predstavljata preverjevalec in registrator. Preverjevalec in registrator sta elektronska, načeloma bi lahko bila tudi realni osebi.
Predstavitev sheme po točkah, kot so označene na sliki:

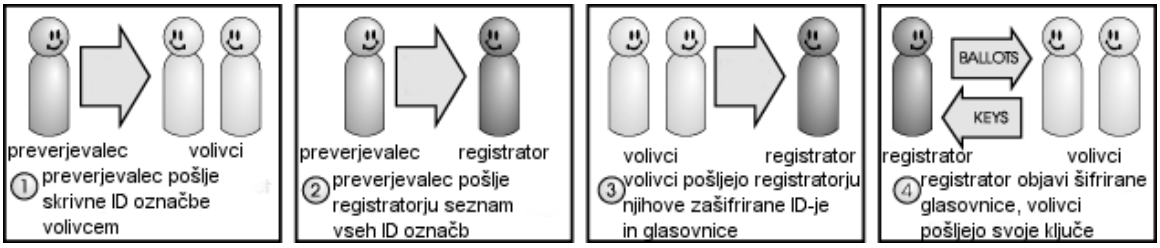
1. Volivec svojo elektronsko glasovnico skupaj z svojo identifikacijsko številko pošlje preverjevalcu.
2. Ta uporabi identifikacijsko številko za to, da preveri ali oseba lahko glasuje in še ni glasovala. Če sta ta dva pogoja izpolnjena, označi, da je oseba volila. Preverjevalec ne odpre glasovnice in tako ne vidi, kako je konkretni volivec glasoval.
3. Če je vse v redu pošlje samo glasovnico, brez identifikacijske številke, naprej registratorju. Registrator prejeme od preverjevalca le glasovnico, brez identifikacijske številke in tako ne more vedeti, od katerega volivca je ta glasovnica. Registrator prejeto glasovnico odpre in glas ustrezno registrira oziroma ga šteje pod pravo izbiro.

Kljub nekaterim dobrim lastnostim, ima shema kar nekaj pomanjkljivosti. Nič nam ne zagotavlja, da preverjevalec res ne prebere glasovnice. Volivec lahko odda glas z identifikacijsko številko nekoga drugega, še več, lahko odda celo več glasov. Naprej nimamo zagotovila, da preverjevalec in registrator ne spreminjata glasovnice. Volivec se tudi ne more prepričati ali je bil njegov glas pravilno upoštevan. Tako preverjevalec kot registrator lahko dodajata glasove po želji. Ni težko najti še vrsto drugih problemov in pomanjkljivosti.

Tako je ta shema v praksi popolnoma neuporabna. Nekatere opisane probleme rešuje naslednja shema.

4.1.2. Shema z dvema agencijama

Tudi za to shemo je najprej podana slika:



Slika 2: Shema z dvema agencijama

Pričujočo shemo so predlagali Nurmi, Salomaa in Santean.

Predstavitev sheme po točkah, kot so označene na sliki:

1. Elektronski preverjevalec še pred volitvami razpošlje volivcem skrivno identifikacijsko označbo.

2. Poleg tega preverjevalec pošlje seznam vseh teh razposlanih skrivnih označb tudi registratorju, vendar le seznam, tako, da registrator ne ve kateremu volivcu pripada katera oznaka.
3. Volivec pri glasovanju pošlje registratorju svojo identifikacijsko oznako in zašifrirano datoteko, ki vsebuje identifikacijsko oznako in glasovnico. Tako se lahko na podlagi identifikacijske oznake registrator prepriča, da je glas veljaven, ne more pa pogledati glasovnice, saj je ta zašifrirana.
4. Registrator javno objavi zašifrirano datoteko, tako, da volivec vidi, da je bila njegova glasovnica prejeta. Ko volivec to vidi, pošlje registratorju ključ za odšifriranje poslane datoteke. Po koncu volitev registrator objavi listo vseh glasovnic in njim ustreznih zašifriranih datotek.

Tako se lahko volivci prepričajo, da je bil njihov glas pravilno upoštevan. Če ugotovijo napako, lahko protestirajo, napako lahko dokažejo tako, da še enkrat pošljejo zašifrirano datoteko in dešifrirni ključ. Ker je bila glasovnica že prej javno objavljena, registrator ne more zanikati njenega prejetja. Privatnost je še vedno zagotovljena, saj registrator ne more povezati volivca z glasovnico.

Shema je veliko boljša od prejšnje, vendar ima še vedno pomanjkljivosti. Če preverjevalec in registrator sodelujeta, lahko povežeta volivca z njegovim glasom. S tega stališča avtorji predlagajo poenostavitev iz dveh agencij na eno samo.
Drugi problem pri tej shemi je, da lahko volivci nekomu tretjemu dokažejo kako so volili, saj imajo šifrirano datoteko in dešifrirni ključ. S tem je omogočeno izsiljevanje in kupovanje glasov.
Tretji problem je v tem, da ima registrator seznam vseh skrivnih oznak, kar lahko tik pred koncem volitev izrabi za oddajo glasov z skritimi oznakami volivcev, ki niso oddali svojega glasu. To lahko ti volivci sicer zaznajo, ne morejo pa dokazati, da niso volili.

Tako tudi ta shema še vedno ne ustreza zahtevam in tako ni preveč uporabna.

V nadaljevanju sledi predstavitev treh tipov kriptografskih volilnih shem.

4.2. Sheme na osnovi Slepega podpisa in Anonimnega kanala

Najprej je treba povedati, kaj sploh je **slepi podpis** in kaj je **anonimni kanal**.

Slepi podpis [9] (stran 475)
Ideja: Pri slepem podpisu želimo imeti podpisano neko sporočilo, brez da bi komurkoli, tudi podpisovalcu razkrili vsebino sporočila. Poleg tega mora biti sporočilo možno podpisati le podpisovalcu, kar mora imeti možnost preveriti vsakdo. Spodaj je podan postopek slepega podpisovanja z RSA kriptografijo.
Vhod: *Podpisovalec*: javni ključ (*n*, *e*) in ustrezen privatni ključ *d*. *Stranka* (tisti, ki zahteva podpis): sporočilo *m*, katerega želi podpisati.
Postopek: 1. Stranka svoje sporočilo *m* najprej zamaskira takole: $m' = mr^e \ mod \ n$, kjer je *r* naključno izbrano število. Tako zamaskirano sporočilo *m′* pošlje podpisovalcu. 2. Podpisovalec podpiše sporočilo *m′* takole $s' = m'^d \ mod \ n$ in pošlje podpisano sporočilo *s′* nazaj stranki. 3. Ta iz *s′* dobi želeno podpisano originalno sporočilo $s = s'/r$.
Izhod: Podpisano sporočilo *s*

Anonimni kanal [4] (stran 9)
Definicija: Anonimni kanal je komunikacijski kanal, pri katerem sprejemnik ne more določiti izvora prejetih sporočil. To se pri e-glasovanju s pridom uporablja za dosego zasebnosti. Sama izvedba anonimnega kanala zna biti precej zapletena. Za razliko od slepega podpisa, kjer je že vse dognano, anonimni kanal ni tako enostavno izvesti.

V grobem sheme na podlagi slepega podpisa in anonimnega kanala delujejo takole:
Volivec od oblasti-administratorja dobi žeton, na podlagi katerega lahko glasuje. Ta žeton je v resnici s strani oblasti slepo podpisano volivčevo sporočilo. To pomeni, da pri konstrukciji žetona sodelujejo oblasti in je tako zagotovljeno, da volivec dobi največ en žeton. Volivec pošlje svoj glas skupaj z žetonom oblasti-zbiralcu zašifrirano po anonimnem kanalu. Oblasti-zbiralci zbirajo te prejete glasove in jih javno objavijo skupaj z žetoni. Tako se lahko volivec najprej prepriča ali je njegov glas pravilno upoštevan in šele nato pošlje zbiralcu ključ z katerim ta odklene glasovnico.

To je le osnovna shema na podlagi slepega podpisa in anonimnega kanala, ki ima svoje pomanjkljivosti:

- oblast-zbiralec ve vmesni rezultat pred koncem volitev,
- pri konstrukciji žetona si volivec sam izmisli sporočilo in si tako lahko dva volivca izbereta enako sporočilo,
- oblast-administrator lahko odda glasove namesto ljudi, ki se volitev ne udeležijo, lahko nekaterim volivcem da več žetonov,
- volivec ne more dokazati neupoštevanja svojega glasu brez razkritja svoje odločitve.

V nadaljevanju sledijo bolj izpopolnjene sheme.

4.2.1. FOO Shema

FOO shema [5] (stran 29) je prva praktično uporabna shema na podlagi slepega podpisa in anonimnega kanala. Njeni avtorji so Fujioka, Okamoto in Ohta, shemo so predstavili na konferenci AUSCRYPT'92 pod naslovom *A practical secret voting scheme for large scale elections*.

Shema uporablja **bit commitment** mehanizem [5] (stran 19). Ta mehanizem v osnovi omogoča prvi osebi pošiljanje enega bita drugi osebi tako da druga oseba na začetku ne vidi vrednosti tega bita, hkrati pa tej drugi osebi zagotavlja, da prva oseba ob poznejšem razkritju vrednosti bita ne more prikazati drugačne vrednosti, kot jo je izbrala na začetku.

FOO shema
Udeleženci: - oblasti administratorji - odgovorni za izdajo žetonov, - oblasti zbiralci, ki zbirajo glasove in na koncu objavijo rezultat volitev, - volivci
Volilni proces poteka v naslednjih fazah: **1. Priprava** Administrator generira shemo za slepo podpisovanje in objavi javni ključ. **2. Registracija** a. **Glasovnica volivca** Volivec se odloči kako bo glasoval in izdela svojo glasovnico (pri

tem uporabi še bit commitment mehanizem, ki preprečuje, da bi kdo njegovo odločitev videl, hkrati pa preprečuje, da bi se volivec kasneje premislil). Tako dobi sporočilo m, katerega zamaskira v m', ga podpiše s svojo identifikacijsko številko in pošlje administratorju v podpis.

b. **Preverjanje in podpisovanje**

Administrator preveri ali je volivčev podpis pravi, ali ima ta volivec pravico voliti in ali ta volivec že ni zaprosil za podpis. Če so vsi pogoji izpolnjeni, administrator podpiše volivčevo sporočilo in ga pošlje volivcu.

c. Objava

Na koncu faze registracije administrator objavi število volivcev, katerim je izvedel podpis in za vsakega tega volivca trojico (identifikacijska številka, podpisana volivčeva glasovnica, zamaskirana volivčeva glasovnica).

3. Glasovanje

a. Volivčevo preverjanje

Volivec pregleda administratorjev podpis na prejeti glasovnici.
Če je podpis napačen, volivec lahko protestira, pri čemer lahko pokaže, da vrnjeno podpisano sporočilo ni njegovo sporočilo podpisano z administratorjevim podpisom.

b. Pošiljanje glasu

Če je vse v redu, pošlje podpisano glasovnico anonimno zbiralcu.
Zbiralec ravno tako preveri administratorjev podpis. Če je podpis v redu, zbiralec uvrsti na listo trojko (zaporedna številka, originalna glasovnica pred maskiranjem, podpisana glasovnica od administratorja)

4. Štetje

a. Odpiranje

Ko so vsi volivci volili, zbiralec objavi svojo listo omenjenih trojk.
Volivec preveri ali je število glasovnic na zbiralčevi listi res enako številu volivcev.
Volivec preveri ali je njegova glasovnica na listi.
Volivec pošlje zbiralcu dvojico (ključ, zaporedno številko svoje glasovnice na zbiralčevi listi) po anonimnem kanalu.

a. Štetje

Zbiralec z ključem odklene glas pod ustrezno poslano številko in preveri ali je glasovnica pravilno izpolnjena.
Zbiralec prešteje glasove in objavi rezultat.

Analiza sheme po posameznih zahtevah glasovanja:

- **Kvalifikacija**
  Samo resnični volivci lahko glasujejo, ker lahko samo ti pridejo do žetona in lahko ta žeton uporabijo le enkrat. Neveljavni žetoni in glasovi se ne morejo upoštevati, ker se izvajajo ustrezna preverjanja.

- **Zasebnost**
  Zasebnost je popolnoma zagotovljena, tudi če administrator in zbiralec sodelujeta. Povezava med volivčevo identifikacijsko številko in njegovo glasovnico ni možna zaradi slepega podpisa. Volivec pošlje svojo glasovnico in kasneje ključ za odklepanje glasu po anonimnem kanalu in se ga tako ne da povezati z glasovnico.

- **Preverljivost**
  Vsak volivec lahko preveri svojo glasovnico. Če ugotovi neskladje, lahko to dokaže brez da bi pri tem izdal svojo dejansko odločitev.
  Neodvisno globalno preverjanje pri tej shemi ni izvedljivo. Administator lahko tako odda glasove za tiste, ki se niso udeležili volitev oziroma faze registracije.

- **Pravičnost**
  Štetje glasov se izvede po koncu volitev.

- **Odsotnost potrdila**
  Volivec ima pri sebi žeton, s pomočjo katerega lahko vsakdo ugotovi kako je volil. Tako odsotnost potrdila ni dosežena.
  Problem odsotnosti potrdila se da popraviti z manjšo spremembo.

4.3. Sheme na osnovi Homomorfne enkripcije

Te sheme uporabljajo **homomorfno enpripcijo** in shemo za **deljenje skrivnosti**.

Homomorfna enkripcija [4] (stran 7)
Definicija: Imejmo operacijo $\oplus$ definirano nad množico čistopisov in operacijo $\otimes$ definirano nad množico tajnopisov. Homomorfnost pomeni, da je 'produkt' poljubnih dveh zašifriranih čistopisov m_1 in m_2 , torej $E(m_1) \otimes E(m_2)$ enak zašifrirani 'vsoti' teh dveh čistopisov, torej $E(m_1 \oplus m_2)$.

Deljenje skrivnosti [5] (stran 14)
Definicija: Izbrano skrivnost želimo deliti med N osebami tako, da lahko pridejo do skrivnosti samo neke koalicije teh oseb. Ponavadi je to neko število t < N teh oseb. Koaliciji manj kot t oseb ne sme uspeti priti do varovane skrivnosti.

Pri homomorfnih shemah gre poenostavljeno povedano za naslednjo idejo: volivec svoj glas razdeli na N delov in vsak del pošlje eni od N oblasti, zašifriran z ključem te oblasti. Oblasti na podlagi homomorfne lastnosti izračunajo vsaka svoj del in te dele objavijo. Rezultat volitev so vsi ti deli skupaj. Volitve uspejo le, če je vnaprej določeno število t oblati poštenih.

4.3.1. Benaloh-ova shema

Ta shema uporablja zgoraj omenjeno **homomorfno enkripcijo** in **deljenje skrivnosti**. Uporabna je le za najosnovnejši da/ne tip volitev.

Benaloh-ova shema
Udeleženci: - *N* predstavnikov oziroma grup oblasti, - volivci
Volilni proces poteka v naslednjih fazah: **1. Priprava** Vsaka oblast *Aj* si pripravi svojo instanco javne kriptografije. **2. Glasovanje** Volivec si izbere par glasov (v_1, v_2) tako, da permutira (0, 1). Volivec v_1 in *v2* razbije na *j* delov: $v_1 = (s_1(v_1),... s_N(v_1))$, enako *v2*. Volivec zašifrira *j*-ti del z ključem *j*-te oblasti in tako dobi par $h=(h_1, h_2)$

$h_i=(h_{i1},\ldots, h_{iN})$, $i=1, 2$
$h_{ij}=E_j(s_j(v_i))$, $j=1,\ldots,N$

Volivec objavi h in dokaže oblasti, da je h pravilno konstruiran.
Ta dokaz je poseben postopek.
Volivec izbere h_1 ali h_2 kot svojo odločitev.

3. **Štetje**
   Če se je volivec odločil za npr. $h_1=(h_{11},\ldots, h_{1N})$, potem j-ta oblast z uporabo homomorfne lastnosti izračuna:

$$\prod_{i=1} h_{ij} = \prod_{i=1} E_j(s_j(v_i)) = E_j(\sum_{i=1} s_j(v_i))$$

   Oblast j dešifrira vsoto vseh svoji delov (ta vsota je $S_j = \sum_i s_j(v_i)$). S_j skupaj z dokazom o pravilnem dešifriranju javno objavi.

   Če to uspe podmnožici A vsaj t+1 od N-tih oblasti, lahko izračunamo končno vsoto glasov

$$S = \sum_{j\in A} S_j \lambda_j = \sum_{j\in A}(\sum_i s_j(v_i))\lambda_j = \sum_i \sum_{j\in A} s_j(v_i)\lambda_j = \sum_i v_i$$

   kjer so λ_j koeficienti Lagrange-ove interpolacije. Lagrengeova interpolacija je del Shamir-jeve sheme za delitev skrivnosti; uporabimo jo, da iz j delov skrivnosti sestavimo nazaj celo skrivnost.

Analiza sheme po posameznih zahtevah glasovanja:

- **Kvalifikacija**
  Glasujejo lahko le volivci, ki imajo pravico glasovati in ti le enkrat. To se preverja v fazi glasovanja, kjer mora vsak volivec dokazati pravilnost konstruiranja $h=(h_1, h_2)$

- **Zasebnost**
  Zasebnost volivca je varovana z šifriranjem njegovega glasu. Zasebnost lahko razbije koalicija t oblasti. Ker pa smo postavili predpostavko, da mora biti t od N oblasti zanesljivih, je tako zasebnost ob tej predpostavki dosežena.

- **Splošna preverljivost**
  Vsakdo lahko preveri veljavnost glasov in vsakdo lahko izračuna dele posamezne oblasti in skupen rezultat. Tako je shema popolnoma zunanje neodvisno preverljiva.

Shemo se da razširiti na 1-od-L tip volitev in na utežene volitve.
Vse homomorfne sheme, vključno z predstavljeno zahtevajo veliko komunikacije, saj mora vsak volivec poslati po en del svojega šifriranega glasu vsem n oblastem.

4.4. Sheme na osnovi Mešanja glasov

Osnovna ideja za **sistemom mešanja glasov** je precej enostavna. Možne izbire gredo preko *N* oblasti, vsaka jih permutira in to permutacijo razkrije le volilvcem. Volivec izbere glas iz rezultata vseh teh permutacij. Le vse oblasti skupaj lahko ugotovijo pravi glas volivca.

Shema z mešanjem glasov
Postopek (za 1-od-*L* volitve): Pri teh volitvah nastopa *N* oblasti A_1 do A_N. *L* možnih izbir je na začetku urejenih v nek seznam. Nato vsaka oblast A_j ta seznam permutira na nek naključen način in seznam ponovno zašifrira. To permutacijo seznama pošlje le volivcu. Seznam pošlje naprej naslednji oblasti, ki seznam spet permutira in zašifrira, ter pošlje permutacijo volivcu po kanalu, kateremu se ne da prisluškovati in spremenjen seznam naslednji oblasti. Pri zadnji oblasti dobimo končen seznam. Tako imamo *N* oblasti, od katerih vsaka ve le za svojo permutacijo poleg tega pa še volivce, ki vedo za vse permutacije. Posledično iz tega le volivec ve preslikavo začetnega seznama možnosti v končni seznam. Volivec se odloči za svojo izbiro in jo permutira po vseh zaporednih permutacijah. Oblasti lahko na koncu le z skupnim sodelovanjem odpermutirajo in odšifrirajo posamezen glas. Ti dve operaciji seveda potekata ravno v obratnem vrstnem redu. Če je uporabljeno homomorfno šifriranje, se glasovi seštejejo po homomorfnem pravilu: vsi šifrirani glasovi se zmnožijo in odšifrirajo.

Shema zagotavlja dobro zasebnost, robustnost, je univerzalno preverljiva, ne da se dokazati kako je kdo volil. Vse te lastnosti seveda slonijo na predpostavki ustreznosti uporabljene kriptografije in kanala za komunikacijo z volivcem.

5. IZVEDLJIVOST I-GLASOVANJA

V tem poglavju iščem odgovor na vprašanje, ali so dandanes izvedljive volitve preko Interneta. Večino ugotovitev se da posplošiti na splošno (elektronsko) oddaljeno glasovanje.

I-Glasovanje je zanimivo predvsem zaradi svoje prikladnosti. Volivcem ne bi bilo treba več iti na volišče, ampak bi lahko glasovali kar od doma ali od kjerkoli drugje. To pomeni manjšo porabo časa in možnost glasovanja od kjerkoli.

Pri I-Glasovanju se moramo spopasti z nekaterimi problemi, večina teh problemov je že bila omenjena pri problemih oddaljenega dostopa:

- izsiljevanje,
- kupovanje glasov,
- registracija volivcev.

Registracija volivcev je problem zase, katerega je danes še težko zadovoljivo rešiti. Registracija je splošen problem Interneta.

Za I-Glasovanje bodo ljudje uporabljali svoje domače računalnike in brskalnikov. Tako lahko za analizo izvedljivosti izberemo kar vsem dobro poznane PC računalnike z najbolj razširjenimi operacijskimi sistemi in brskalniki, ki so v Internet povezani preko TCP/IP omrežja.

5.1. Zlonamerna koda

Prva nevarnost in ovira za izvedbo I-Glasovanja danes je zlonamerna koda. Vsak uporabnik računalnikov se dnevno otepa raznih virusov, črvov in podobnih škodljivih programov, katere imenujemo zlonamerna koda.
Bistvo problema zlonamerne kode je, da je možno napisati program, ki se lahko preko Interneta precej generalno razširi in katerega se ne more nobeden ubraniti. Dokaz za to so novi in novi virusi in druge oblike zlonamerne kode. Ta problem postane še bolj kritičen ob dejstvu, da lahko ta koda naredi na računalniku neomejeno količino škode oziroma lahko počne karkoli.
Tako bi lahko napisali program, ki bi volivčev glas pred npr. šifriranjem prestregel in ga spremenil. Tak program bi tako spremenil volilni program, da bi uporabnikov vnos spremenil in poslal naprej, uporabniku pa še vedno na zaslonu prikazal njegov glas. Škodljiv program bi se lahko po volitvah odstranil in se tako ne bi dalo dokazati, da je sploh kdaj bil na računalniku.

Že nekaj časa obstajajo programi, ki omogočajo oddaljeno delo na računalniku (npr. PC Anywhere, WinXP Remote Desktop Connection). Podobno imamo programe za oddaljen nadzor, kot je Backorifice 2000 (http://www.bo2k.com), s katerim lahko spremljamo uporabnikove akcije in poljubno upravljamo z vsemi viri računalnika (tipkovnica, …).

BO2K dela v prikritem načinu in je tako dobro napisan, da ga imajo težavo odkriti tudi izkušeni administratorji (proces ni viden niti v seznamu aktivnih procesov). BO2K je open source projekt in ga tako lahko vsakdo dobi in prilagodi za zlonamerne namene.
Naprej imamo že veliko časa viruse, ki se sprožijo na določen dan. Taka sprožitev zelo razširjenega virusa lahko zaustavi delovanje kar konkretnega dela Interneta. Ker je dan volitev znan kar precej vnaprej, bi lahko nekdo napisal virus, ki bi na ta dan onemogočil veliko računalnikov in tako onemogočil oddajo glasov delu volivcev.
Naprej lahko z nastavitvijo ti. proxy nastavitev napadalec preusmeri komunikacijo volivca iz volilnega strežnika nase.

Tudi razširjanje takšne zlonamerne kode je možno izvesti precej učinkovito. Lahko bi uporabili dejstvo, da računalniki doma večino časa niso varovani. Ampak zakaj bi zlonamerno kodo razpečevali na tako zapleten način, če lahko to naredi ta koda avtomatično. Lep primer so spet računalniški virusi, ki uspejo v enem dnevu okužiti na milijone računalnikov. Načini razširjanja so že tako razviti, da je dovolj le, da je računalnik priključen na Internet; niti ni treba odpreti pošte ali kaj podobnega.

5.2. Komunikacijska infrastruktura

V prejšnjem poglavju smo si ogledali napade na računalnike volivcev. Poleg teh imamo še volilne strežnike in povezave med volilnimi strežniki in računalniki volivcev. Tu se pojavi spet kup problemov. Za samo zaščito podatkov lahko učinkovito uporabimo kriptografijo; problem je zagotoviti volivcem dostopnost do volilnih strežnikov.

Najbolj znan napad je zanikanje storitve (denial of service). Pri tem napadu na nek strežnik pošljemo tako veliko število zahtev, da jih ne more sproti obdelati in ga tako naredimo nedostopnega. Da se narediti tudi porazdejeno varianto takega napada, pri kateri pred napadom instaliramo napadalne programe na več računalnikov po Internetu in te programe tempiramo tako, da se sprožijo hkrati ob določnem datumu in uri.
Programe oziroma skripte za take napade lahko dobi vsakdo brezplačno na Internetu. Njihova uporaba je zelo enostavna, tako, da je za tak napad potrebno zelo malo znanja.
Drugi tak napad je napad na DNS strežnike, kjer lahko onemogočimo izbrane domene uporabnikov. Znan je še napad, pri katerem pošljemo računalniku v več paketih sporočilo, ki je zanj preveliko. Lista možnih napadov se tu seveda ne konča, vsake toliko časa pa se še dopolni z novimi idejami.

5.3. Neusposobljenost uporabnikov

Veliko uporabnikov se da prepričati, da nam izdajo določeno informacijo, katero lahko izkoristimo za onemogočanje ali spreminjanje njihovega glasu.

Večina uporabnikov ima probleme že z najbolj osnovnimi računalniškimi operacijami. Problem je tudi razumevanje navodil in uporabniškega vmesnika glasovanja.

5.4. Končna ugotovitev

Vsi našteti problemi imajo še večjo težo zato, ker se pojavijo globalno. Pri neoddaljenih volitvah imamo več geografskih enot in pod enot. Do napak in goljufij lahko pride le v eni ali več enotah, učinki nepravilnosti ene enote pa se ne širijo na druge. Pri splošnem oddaljenem glasovanju je možnost širše zlonamerne dejavnosti večja, pri I-Glasovanju pa je to delovanje kar avtomatsko globalno.
Treba se je zavedati, da viruse in podobne programe pišejo doma ljudje najstniki za zabavo. Kakšne so šele motivacija in zmožnosti nekoga, ki bi s tem lahko spremenil izid volitev.

Iz vsega povedanega sledi, da volitve preko Interneta dandanes niso izvedljive. Rešiti bi morali vse naštete probleme, kar pa se ne da storiti čez noč.
Problema zlonamerne kode ne bo nikoli možno rešiti v celoti, dalo pa bi se veliko narediti z reševanjem lukenj v operacijskih sistemih oziroma z implementacijo varnejših standardov in arhitektur. Drugače rečeno, teorija ponuja dobre pristope, ki v praksi niso dobro implementirani.
Problemov komunikacijske infrastrukture je več vrst. Zagotavljanje zadostnih kapacitet je relativno enostaven in rešljiv tehnični problem. Zaščita podatkov je dobro rešena z uporabo kriptografije. Večji problem so razni napadi v smislu onemogočanja storitev ali zasedanja kapacitet, kjer je ena možna rešitev vpeljava novih mehanizmov, ki bi take napade preprečevali. Največji problem ostaja zaupna pot (trusted path) med uporabnikom in volilnim strežnikom.
Pomembno vlogo ima usposabljanje uporabnikov za uporabo volilnih sistemov preko Interneta. Še bolj pomembno kot razlaga detajlov tehnične uporabe teh sistemov, pa se mi zdi ljudem razložiti neustreznost tradicionalnih volitev ter prednosti in izboljšave, ki jih nudijo volitve preko Interneta oziroma sodobne volilne sheme na splošno.

Seveda obstaja tudi nekaj alternativnih rešitev. Del teh problemov bi lahko rešili z posebnimi elektronskimi napravami. Na primer z pametnimi karticami, na katerih bi bili shranjeni podatki o volivcu in bi znale izvajati volilne sheme. Te kartice bi lahko imele tudi nek vmesnik, za vnos izbire. Vendar to še vedno ne reši vseh komunikacijskih problemov.
Poleg računalnikov ima danes večina ljudi telefone in bi morda lahko te prilagodili za glasovanje. Taki poskusi že obstajajo, en tak primer je evropski projekt Cybervote, kateri je opisan v naslednjem poglavju.

I-Glasovanje se že uporablja v nekaterih organizacijah za manj pomembne odločitve, kjer zasebnost in druge zahteve glasovanja niso tako pomembne. Uporaba I-Glasovanja za volitve na državni ravni pa še lep čas ne bo realnost.

6. E-GLASOVANJE PO SVETU

Najbolj zanimiva država glede glasovanja so definitivno **ZDA**, predvsem zaradi raznolikosti sistemov in naprav za glasovanje in njihovih poizkusov testno izvesti napredne volitve v praksi (glej drugo poglavje o zgodovini sistemov za glasovanje).
Leta 1975 so končno začeli pravilno razmišljati in je takratni National Bureau of Standards izdelal poročilo *Effective Use of Computing Technology in Vote-Tallying*, bolj oceno stanja, kot možnosti, kjer so ugotovili, da imajo pomanjkljivo opremo in znanja. Do leta 1984 so izdelali poročilo o izvedljivosti razvoja standardov za volitve in opremo (*A Report on the Feasibility of Developing Voluntary Standards For Voting Equipment*). Do leta 1990 so izdelali standarde za luknjane kartice, zaznavo oznak in DRE (Direct Recording Electronic).

V **Evropi** so se stvari odvijale podobno, le manj odmevno in morda malo bolj premišljeno. Vsaka večja država je tako ali drugače poskušala po svoje izboljšati proces glasovanja.
Najpomembnejši projekt v Evropi pa je leta 2000 začela Evropska komisija. Projekt se je imenuje CyberVote [7] , končal se je septembra 2003. Namen CyberVote projekta je bil ugotoviti možnosti elektronskih in oddaljenih volitev, ter izdelava prototipa. Projekt zajema vse aspekte glasovanja, od tehničnih do pravnih. Kot tipa oddaljenega dostopa so izbrali Internet in mobilne telefone.
Začetno načrtovani projekt je sedaj zaključen. Izvaja se veliko testiranj na manjših območjih, npr.mestih.

Z kriptografskega in izvedbenega stališča projekt podaja kar nekaj predlogov. Za avtentikacijo preko telefonov predlagajo PIN kodo. Za Internetne volitve ocenjujejo kot najbolj primerno SSL tehnologijo, preko katere poteka vsa komunikacija, od prejetja volilne programske opreme do oddaje in preverjanja glasu. Kot največja nerešena problema do sedaj implementiranih in izvedenih Internetnih volitev izpostavljajo zasebnost odločitve volivca in možnost nadzora pravilnosti volilnega procesa.

Predlagana shema uporablja naslednje koncepte: oglasno desko, ElGamalov kriptosistem, delitev skrivnosti, podpisovanje in homomorfnost.
V shemi nastopajo volivci, oblasti, ki upravljajo z oglasno desko, oblasti-števci glasov in pregledovalci-sestavljalci končnega rezultata.
Pred volitvami se vzpostavi ena ali več oglasnih desk, naredi se register volivcev in register oblasti, ki štejejo glasove, volivci in oblasti-števci registrirajo svoje javne ključe na oglasni deski. Na koncu se stanje zamrzne, vse te informacije so vidne vsem.
Volivci oddajo dele svojih glasov, podpisanih s svojim javnim ključem različnim oblastem-števcem. Oblasti-števci po vseh oddanih glasovih zamrznejo stanje, s tem dosežejo konec oddajanja glasov. Oblasti-števci izračunajo svoje delne vsote in jih objavijo na oglasni deski. Pregledovalci oziroma sestavljalci končnega rezultata najprej preverijo ustreznost vseh objavljenih podatkov ter sestavijo in objavijo končni izid volitev.

Zanimiva značilnost opisane sheme je, da volivci pri oddajanju delov glasu niso anonimni, kar sploh ni problem, saj morebitni napadalec vidi le dele volivčevega glasu, kar mu nič ne koristi, saj iz njih ne more sestaviti celotnega glasu.

V **Sloveniji** je očitno usoda E-Glasovanja predvsem v rokah politike, ki ne kaže večjega zanimanja. Namenili so se počakati na uveljavitev E-Glasovanja po svetu, kar morda sploh ni slab pristop, še posebej za tako majhno državo.

7. ZAKLJUČEK

Dandanes je sistem glasovanja še v razvoju. Zahteve in lastnosti idealnega glasovalnega procesa so dobro definirane, idealne glasovalne sheme, ki bi tem zahtevam ustrezala, pa še ni ne v teoriji, ne v praksi.
Vendar se stvari počasi premikajo naprej in tako počasi dobivamo vse boljše sheme, pravne predpise in vse drugo potrebno.
Tradicionalne volitve, v primerjavi z najnovejšimi dognanji, precej slabo pokrivajo zahteve dobrega glasovanja. Tako bi moral biti današnji cilj, poleg teoretičnih raziskav, aktivna implementacija in uporaba najnovejše teorije v praksi.
Varno in vsem zahtevam glasovanja ustrezno I-Glasovanje je dandanes neizvedljivo zaradi problemov oddaljenega dostopa in narave Interneta samega, še posebej zaradi globalnosti. Podobno velja za vse druge tipe oddaljenega dostopa.
Treba se je zavedati koristi, ki ga prinese goljufanje pri volitvah, in s tem motivacije napadalcev vplivati na izid volitev.

Seveda pa je prihodnost glasovanja očitno ravno v E-Glasovanju oziroma oddaljenemu glasovanju in podpori z računalniki in kriptografijo.

8. REFERENCE

[1] Mary Bellis, History of voting Machines
http://inventors.about.com/library/weekly/aa111300b.htm

[2] Lorrie Faith Cranor, Electronic Voting: Computerized pools may save money, protect privacy, ACM Inc, 1996
http://www.acm.org/crossroads/xrds2-4/voting.html

[3] Florence Fowler, Computer and Network Security: Internet Voting, University of Tennessee, Knoxville, 2003
http://www.cs.utk.edu/~ffowler/cns-html/project.html

[4] Mike Burmester, Emmanouil Magkos, Doktorat: Advances in Information Security - Secure Electronic Voting: Towards secure and practical e-elections in the new era, Kluwer Academic Publishers pp. 63-76, 2003
http://thalis.cs.unipi.gr/~emagos/overview_voting_2002.pdf

[5] Zuzana Rjaškova, Diplomska naloga: Electronic Voting Schemes, Department of Computer Science, Faculty of Mathematics, Physics and Informatics, Comenius University, Bratislava, April 2002
http://www.ksp.sk/~zuzka/elevote.pdf

[6] Avi Rubin, Security Considerations for Remote Electronic Voting over the Internet, AT&T Lavs – Research, November 1998
http://avirubin.com/e-voting.security.html

[7] CyberVote
http://www.cybervote.org

[8] Gregor Cerar, Elektronska demokracija, Mladina, Januar 2004
http://www.mladina.si/tednik/200404/clanek/uvo-manipulator--gregor_cerar-2/

[9] A. Menezes, P. Van Oorschot, S. Vanstone: Handbook of Applied Cryptography, CRC Press, 1996